REMARKS/ARGUMENTS

Applicants thank the Examiner for the Examiner Interview.

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application fail to comply with 35 USC § 112, second paragraph, and that none of the claims now pending in the application are obvious under the provisions of 35 USC § 103 (a). Thus, the Applicants believe that all of these claims are now in allowable form.

Reexamination and reconsideration of the application are respectfully requested. If, however, the Examiner believes that there are any unresolved issues in any of the claims now pending in the application, Applicants request that the Examiner telephone Ms. Janet M. Skafar, Esq. at telephone number (650) 988-0655 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Status of Claims

Claims 7-11, 15-19, 29-34, 37-42, 47, 48-49, 50-65 are pending in this application. Claims 7-11, 15-19, 29-34, 37-42, and 48-49 are amended. Claims 1-6, 12-14, 20-28, 35, 36, and 43-45 are canceled. Claims 50-65 are new.

Amendments to the Specification

Applicants have amended the paragraph of the specification on page 4, starting at line 8 to delete the phrase "the data can be repaired and". Applicants believe that no new matter has been added.

Claim Rejections under 35 U.S.C. § 112

Claims 1-6, 23-28 and 37 are rejected under 35 USC § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Because Applicants have canceled Claims 1-6 and 23-28, Applicants submit that the rejection with respect to Claims 1-6 and 23-28 is now moot, and request that the rejection be withdrawn.

Applicants have amended Claim 37 with respect to the term data element. Therefore, Applicants respectfully request that the rejection of Claim 37 be withdrawn.

NOTIFICATION OF BROADING OF CLAIMS

Applicants hereby notify the Examiner that Applicants are broadening the claims. Applicants hereby retract all prior arguments in all prior amendments distinguishing the claimed invention from the prior art. Any disclaimer that may have occurred during the prosecution of this patent application is hereby expressly rescinded. Applicants respectfully invite the Examiner to reconsider previous rejections and art with respect to the broader claims.

Applicants point out that the claims have been amended to more broadly recite a "first key" and a "second key" rather than a "static key" and a "dynamic key", respectively.

As to Claim 7, Applicants point out that the following recitations have been deleted: "wherein said encrypting maintains an"; "decrypting said encrypted data element with said static key and said dynamic key on said receiving computer system", and "determining whether transmission of a previous encrypted data element failed; and", and "in response to said determining said transmission of said previous encrypted data element failed,".

As to Claim 15, Applicants point out that the following recitations have been deleted: "wherein said encrypting maintains an encryption state", "decrypting said encrypted data element with said static key and said dynamic key on said receiving computer system;", "determining whether transmission of a previous encrypted data element failed", "in response to said determining said transmission of said previous encrypted data element failed", and "and said dynamic key without retransmission of said previous encrypted data element."

As to Claim 29, Applicants point out that the following recitations have been deleted: "said data element chunks, said static encrypted data element chunks being associated with static encryption states, respectively said static encryption states being used to vary values of said static encrypted data element chunks being statically encrypted with said static key", "data element chunks, respectively", "decrypting said dynamic-static data element chunks with said static key and said dynamic key on said receiving computer system;", "determining, on said receiving computer system, whether transmission of a previous one of said dynamic-static data element chunks failed; and", "in response to said determining said transmission of said previous one of said dynamic-static data element chunks failed," and "one of said dynamic-static data element chunks, wherein said previous one of said dynamic-static data element chunks associated with said failed transmission is not recovered".

As to Claim 37, Applicants point out that the following recitations have been deleted: "wherein said encrypting maintains an encryption state", "decrypting said data element chunks with said static key and said dynamic key on said receiving computer system;", "determining whether transmission of said data element chunks from said second computer system to said receiving computer system failed; and", "in response to said determining said transmission of said one of said dynamic-static data element chunks failed,", and "one or said data element chunks, and said dynamic key without retransmission of said one of said dynamic-static data element chunks associated with said failed transmission".

Claim Rejections under 35 U.S.C. § 103(a)

Claims 1-5, 7-10, 12, 15-18, 20-27, 29-32, 34, 37-40, and 45-49 are rejected as being unpatentable over Mitty et al. US Patent No. 6,145,079 ("Mitty") in view of Shimomura et al U.S. Patent No. 6,473,858 ("Shimomura").

Applicants agree that Mitty does not teach the use of encryption states. The rejection asserts that encrypted information sent with error correction coding teaches said encrypted data being transmitted with said encryption state.

In response to the rejection, the Applicants have also amended claims 7-11, 15-19, 29-34, 37-42, and 48-49 to more particularly point out the invention.

The rejection will be discussed with respect to independent Claim 7.

Applicants respectfully maintain that the combination of Mitty and Shimomura does not teach, expressly or implicitly, all the recitations of the claimed invention. Claim 7 recites: encrypting said data element with said first key and a current encryption state to produce a first encrypted data and an updated encryption state; encrypting said first encrypted data with said second key to produce a second encrypted data; transmitting said second encrypted data with said current encryption state to a receiving computer system; encrypting a subsequent data element with said first key and said updated encryption state to produce a subsequent first encrypted data and a subsequent updated encryption state; encrypting said subsequent first encrypted data with said second key to produce a subsequent second encrypted data; transmitting said subsequent second encrypted data with said updated encryption state to a receiving computer system; decrypting, on said receiving computer system, said subsequent second encrypted data with said second key to produce a decrypted subsequent second encrypted data; and decrypting said decrypted subsequent second encrypted data with said first key and said updated encryption state transmitted with said subsequent second encrypted data to produce a decrypted subsequent data element.

Applicants respectfully maintain that the error correction coding of Shimomura is not the same as the encryption state of the claimed invention. The encryption state of the claimed invention has a different purpose from the error correction code of Shimomura. The encryption state of the claimed invention makes the encryption less susceptible to context-based attacks. The error correction code of Shimomura is to detect and correct errors.

Furthermore, even Shimomura teaches that encryption and error correction are used for different purposes. In col. 6, lines 15-29, Shimomura teaches:

> Data encryption provides several very useful features to the system of the present invention. First, data encryption provides privacy. By encrypting the information streams,

only the desired recipients will be able to read and use an encrypted digital information stream. Encryption can also be used to provide authenticity. For example, an information stream may be encrypted with a private-key in a public-key encryption system such that a recipient can authenticate the identity of the sender by decrypting the message with the alleged sender's public key. One of the most important features that encryption also provides to the present invention is a means of performing access control. Specifically, a set of authorized recipients can be created such that only those recipients can access a particular encrypted digital information stream.

With respect to error correction, in col. 7, lines 45-65, Shimomura teaches:

Since the present invention transmits a digital information stream across a unidirectional broadcast medium, the system of the present invention goes to great lengths to ensure that information that is broadcast will be received intact by the receiver systems. To help obtain this goal, the present invention uses forward error correction. In one embodiment of the present invention, the individual digital information streams are each encoded with a forward error correction (FEC) coding system. By performing the forward error correction coding on an individual digital information stream basis, the present invention can provide different levels of data integrity to the different digital information streams. In this manner, the broadcast facility can charge a higher fee to a customer that requests a very reliable data stream that requires a larger amount of redundant information to ensure data integrity. There are many different well-known forward error correction encoding systems that may be used by the broadcast system of the present invention. In one embodiment, a variation of the well-known Reed-Solomon forward error correction encoding system is used.

In column 13, line 65 to column 14, line 7, Shimomura teaches:

The MPEG-2 frame reassemble places the frames into a defined order such that a forward error correcting code may be used to check for errors and correct detected errors. Thus, at step 925, the control program performs error correction on the reassembled MPEG-2 data frames. The error correction is in addition to the error correction that already exists for MPEG-2 transport streams since the present invention may be used to carry important data that must not be lost or altered.

Thus Shimomura teaches that the error correcting code is used to check for errors and to correct detected errors, and that encryption is used to provide privacy, authenticity and access control. Therefore, even Shimomura teaches that an error correcting code is different from encryption.

For the foregoing reasons, Applicants respectfully maintain that Claim 7 is not obvious and is patentable. Claims 8-10, 12, 46, and 48 depend from Claim 7, and Applicants respectfully maintain that Claims 8-10, 12, 46 and 48 are patentable for the same reasons as Claim 7.

Independent Claims 15, 29 and 37 contain similar distinguishing recitations as Claim 7 and Applicants respectfully maintain that Claims 15, 29 and 37 are patentable for the same reasons as Claim 7. Claims 16-18, 47 and 49; 30-32 and 34; and 38-40 depend from Claims 15 and 37, and Applicants respectfully maintain that Claims 16-18, 47 and 49; 30-32 and 34; and 38-40 are patentable for the same reasons as Claims 15, 29 and 37, respectively.

Claims 10, 18, 32 and 40

Applicants respectfully maintain that Claims 10, 18, 32 and 40 have additional recitations not taught by Mitty or Shimomura. In Claims 10, 18, 32 and 40, the second computer system is untrusted. The rejection asserts that Mitty as modified fails to teach the second computer system being untrusted. The rejection contends that untrusted computers are well known in the art and it would have been obvious to a person of ordinary skill in the art to allow Mitty's system to work with untrusted computers because it offers the advantage of allowing interoperability with a far wider range of networks and systems.

Applicants respectfully disagree. Mitty is directed to secure electronic transactions using a trusted intermediary to perform electronic services. In Claims 10, 18, 32 and 40, the second computer system is untrusted. Unlike Mitty, the claimed invention eliminates the need for a trusted intermediary.

Applicants respectfully maintain that if Mitty used an untrusted intermediary, Mitty would be rendered unsatisfactory for its intended purpose. The invention of Mitty relates to secure electronic transactions, and more particularly, to electronic transactions that use a trusted intermediary to provide improved privacy, authentication, and non-repudiation. (See Mitty, column 1, lines 7-11, and column 2, lines 1-3). Applicants respectfully maintain that modifying Mitty to use an untrusted intermediary in Mitty would not provide improved privacy, authentication, and non-repudiation. Therefore modifying Mitty to use an untrusted intermediary would render Mitty unsatisfactory for its intended purpose of improving improved privacy, authentication, and non-repudiation.

For the foregoing additional reasons, Applicants respectfully maintain that Claims 10, 18, 32 and 40 are not obvious.

Claims 11, 19, 33 and 41

Claims 11, 19, 33 and 41 are rejected as being unpatentable over Mitty in view of Shimomura, and further in view of Bailey III US Patent No. 5,659,614 ("Bailey").

Claims 11, 19, 33 and 41 are dependent on independent Claims 7, 15, 29 and 37, respectively. For all the reasons set forth with respect to independent Claims 7, 15, 29 and 37, Applicants respectfully maintain that neither Mitty nor Shimomura teach all the recitations of Claims 11, 19, 33 and 41. Therefore Applicants respectfully maintain that the combination of Mitty, Shimomura and Bailey does not teach of the recitations of Claims 11, 19, 33 and 41.

For the foregoing reasons, Applicants respectfully maintain that Claims 11, 19, 33 and 41 are not obvious.

New Claims

Applicants have added new claims 50-65.

Applicants point out that in new independent claims 54 and 60, the current encryption state and updated encryption state are part of the recitation of encrypting with the second key. New independent claims 54 and 60 have the recitations of encrypting said first encrypted data with said second key and a current encryption state to produce a second encrypted data and an updated encryption state.

Applicants also point out that Claims 55 and 61 depend from Claims 54 and 60, respectively, and a current first-encryption encryption state and an updated first-encryption encryption state are part of the recitation of encrypting with the first key.

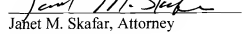
Conclusion

For the foregoing reasons, Applicants believe that the pending Claims 7-11, 15-19, 29-34, 37-42, 47, 48-49, and 50-65 are patentable over the art of record.

Applicants therefore respectfully request that the Examiner reconsider all currently outstanding rejections and that they be withdrawn. It is believed that a full and complete response has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this Application, the Examiner is invited to telephone the undersigned at the number provided. Prompt and favorable consideration of this Response is hereby solicited.

Respectfully submitted,

March 9, 2007



Janet M. Skafar, Attorney
Reg. No. 41,315
Correspondence Customer No. 24852
Telephone: (650)988-0655
Facsimile: (408) 463-4827